§ 543.19 [Reserved]

§ 543.20 What are the minimum internal control standards for information technology and information technology data?

(a) *Supervision*.

(1) Controls must identify the supervisory agent in the department or area responsible for ensuring that the department or area is operating in accordance with established policies and procedures.

(2) The supervisory agent must be independent of the operation of Class II games.

(3) Controls must ensure that duties are adequately segregated and monitored to detect procedural errors and to prevent the concealment of fraud.

(4) Information technology agents having access to Class II gaming systems may not have signatory authority over financial instruments and payout forms and must be independent of and restricted from access to:

(i) Financial instruments;

(ii) Accounting, audit, and ledger entries; and

(iii) Payout forms.

(b) As used in this section only, a system is any computerized system that is integral to the gaming environment. This includes, but is not limited to, the server and peripherals for Class II gaming system, accounting, surveillance, essential phone system, and door access and warning systems.

(c) Class II gaming systems' logical and physical controls. Controls must be established and procedures implemented to ensure adequate:

(1) Control of physical and logical access to the information technology environment, including accounting, voucher, cashless and player tracking systems, among others used in conjunction with Class II gaming;

(2) Physical and logical protection of storage media and its contents, including recovery procedures;

(3) Access credential control methods;

(4) Record keeping and audit processes; and

(5) Departmental independence, including, but not limited to, means to restrict agents that have access to information technology from having access to financial instruments.

(d) *Physical security*.

(1) The information technology environment and infrastructure must be maintained in a secured physical location such that access is restricted to authorized agents only.

(2) Access devices to the systems' secured physical location, such as keys, cards, or fobs, must be controlled by an independent agent.

(3) Access to the systems' secured physical location must be restricted to agents in accordance with established policies and procedures, which must include maintaining and updating a record of agents granted access privileges.

(4) Network Communication Equipment must be physically secured from unauthorized access.

(e) *Logical security*.

(1) Controls must be established and procedures implemented to protect all systems and to ensure that access to the following is restricted and secured:

(i) Systems' software and application programs;

(ii) Data associated with Class II gaming; and

(iii) Communications facilities, systems, and information transmissions associated with Class II gaming systems.

(2) Unused services and non-essential ports must be disabled whenever possible.

(3) Procedures must be implemented to ensure that all activity performed on systems is restricted and secured from unauthorized access, and logged.

(4) Communications to and from systems via Network Communication Equipment must be logically secured from unauthorized access.

(f) *User controls*.

(1) Systems, including application software, must be secured with passwords or other means for authorizing access.

(2) Management personnel or agents independent of the department being controlled must assign and control access to system functions.

(3) Access credentials such as passwords, PINs, or cards must be controlled as follows:

(i) Each user must have his or her own individual access credential;

(ii) Access credentials must be changed at an established interval approved by the TGRA; and

(iii) Access credential records must be maintained either manually or by systems that automatically record access changes and force access credential changes, including the following information for each user:

(A) User's name;

(B) Date the user was given access and/or password change; and

(C) Description of the access rights assigned to user.

(4) Lost or compromised access credentials must be deactivated, secured or destroyed within an established time period approved by the TGRA.

(5) Access credentials of terminated users must be deactivated within an established time period approved by the TGRA.

(6) Only authorized agents may have access to inactive or closed accounts of other users, such as player tracking accounts and terminated user accounts.

(g) *Installations and/or modifications.*

(1) Only TGRA authorized or approved systems and modifications may be installed.

(2) Records must be kept of all new installations and/or modifications to Class II gaming systems. These records must include, at a minimum:

(i) The date of the installation or modification;

(ii) The nature of the installation or change such as new software, server repair, significant configuration modifications;

(iii) Evidence of verification that the installation or the modifications are approved; and

(iv) The identity of the agent(s) performing the installation/modification.

(3) Documentation must be maintained, such as manuals and user guides, describing the systems in use and the operation, including hardware.

(h) *Remote access.*

(1) Agents may be granted remote access for system support, provided that each access session is documented and maintained at the place of authorization. The documentation must include:

(i) Name of agent authorizing the access;

(ii) Name of agent accessing the system;

(iii) Verification of the agent's authorization;

(iv) Reason for remote access;

(v) Description of work to be performed;

(vi) Date and time of start of end-user remote access session; and

(vii) Date and time of conclusion of end-user remote access session.

(2) All remote access must be performed via a secured method.

(i) *Incident monitoring and reporting.*

(1) Procedures must be implemented for responding to, monitoring, investigating, resolving, documenting, and reporting security incidents associated with information technology systems.

(2) All security incidents must be responded to within an established time period approved by the TGRA and formally documented.

(j) *Data backups.*

(1) Controls must include adequate backup, including, but not limited to, the following:

(i) Daily data backup of critical information technology systems;

(ii) Data backup of critical programs or the ability to reinstall the exact programs as needed;

(iii) Secured storage of all backup data files and programs, or other adequate protection;

(iv) Mirrored or redundant data source; and

(v) Redundant and/or backup hardware.

(2) Controls must include recovery procedures, including, but not limited to, the following:

(i) Data backup restoration;

(ii) Program restoration; and

(iii) Redundant or backup hardware restoration.

(3) Recovery procedures must be tested on a sample basis at specified intervals at least annually. Results must be documented.

(4) Backup data files and recovery components must be managed with at least the same level of security and access controls as the system for which they are designed to support.

(k) *Software downloads.* Downloads, either automatic or manual, must be performed in accordance with 25 CFR 547.12.

(l) *Verifying downloads.* Following download of any Class II gaming system software, the Class II gaming system must verify the downloaded software using a software signature verification method. Using any method it deems appropriate, the TGRA must confirm the verification.

§ 543.21 What are the minimum internal control standards for surveillance?

(a) *Supervision.* Supervision must be provided as needed for surveillance by an agent(s) with authority equal to or greater than those being supervised.

(b) *Surveillance equipment and control room(s).* Controls must be established and procedures implemented that include the following:

(1) For Tier A, the surveillance system must be maintained and operated from a secured location, such as a locked cabinet. For Tiers B and C, the surveillance system must be maintained and operated from a staffed surveillance operation room(s).

(2) The surveillance operation room(s) must be secured to prevent unauthorized entry.

(3) Access to the surveillance operation room(s) must be limited to surveillance agents and other authorized persons.

(4) Surveillance operation room(s) access logs must be maintained.

(5) Surveillance operation room equipment must have total override capability over all other satellite surveillance equipment.

(6) Power loss to the surveillance system:

(i) For Tier A, in the event of power loss to the surveillance system, alternative security procedures, such as additional supervisory or security agents, must be implemented immediately.

(ii) For Tier B and C, in the event of power loss to the surveillance system, an auxiliary or backup power source must be available and capable of providing immediate restoration of power to the surveillance system to ensure that surveillance agents can observe all areas covered by dedicated cameras.

(7) The surveillance system must record an accurate date and time stamp on recorded events. The displayed date and time must not significantly obstruct the recorded view.

(8) All surveillance agents must be trained in the use of the equipment, games, and house rules.

(9) Each camera required by the standards in this section must be installed in a manner that will prevent it from being readily obstructed, tampered with, or disabled.

(10) The surveillance system must:

(i) Have the capability to display all camera views on a monitor;

(ii) Include sufficient numbers of recording devices to record the views of all cameras required by this section;

(iii) Record all camera views; and

(iv) For Tier B and C only, include sufficient numbers of monitors to simultaneously display gaming and count room activities.

(11) A periodic inspection of the surveillance systems must be conducted. When a malfunction of the surveillance system is discovered, the malfunction and necessary repairs must be documented and repairs initiated within seventy-two (72) hours.

(i) If a dedicated camera malfunctions, alternative security procedures, such as additional supervisory or security agents, must be implemented immediately.

(ii) The TGRA must be notified of any surveillance system and/or camera(s) that have malfunctioned for more than twenty-four (24) hours and the alternative security measures being implemented.

(c) *Additional surveillance requirements.* With regard to the following functions, controls must also include:

(1) Surveillance of the progressive prize meters for Class II gaming systems at the following thresholds:

(i) Wide area progressives with a reset amount of $1 million; and

(ii) In-house progressives with a reset amount of $250,000.

(2) Manual bingo:

(i) For manual draws, the surveillance system must monitor the bingo ball drawing device or mechanical random number generator, which must be recorded during the course of the draw by a dedicated camera to identify the numbers or other designations drawn; and